PERSEREC

Management Report 01-4
October 2001

Public Opinion of Selected National Security Issues: 1994-2000

Suzanne Wood
Defense Personnel Security Research Center

Defense Personnel Security Research Center
99 Pacific Street, Suite 455-E
Monterey, California 93940-2497

Management Report 01-4 **October 2001**

Public Opinion on Selected National Security Issues: 1994-2000

Suzanne Wood
Defense Personnel Security Research Center

Released by
James A. Riedel
Director

Defense Personnel Security Research Center
99 Pacific Street, Suite 455-E
Monterey, CA 93940-2497

Preface

Since 1994, the Defense Personnel Security Research Center (PERSEREC) has been conducting a longitudinal study of the public's attitudes toward various security policies. This consisted of selected questions being included in four surveys (1994, 1996, 1998 and 2000) that were fielded to a national sample by the National Opinion Research Center (NORC). The people who were questioned in the surveys were not part of the security world. For this very reason, their "outsider" opinions were welcome. Also, ultimately it would be impossible in a democracy to maintain a security system without the support of the general public.

I believe that the results of this extensive study, summarized here, will be of interest to policymakers who shape the way in which personnel security policy is conducted.

James A. Riedel
Director

Table of Contents

Background and Purpose

Security policy is neither developed nor implemented in a vacuum; it exists within a social context. Therefore, it is important to know what the public believes about the subject. For example, does the general public—from whom recruits to the security system are drawn—favor certain security measures? And if not, will those newcomers resent or attempt to undermine a system in which they do not believe?

With the end to the Cold War, counter-espionage needs have become more complex. While traditional espionage challenges have not disappeared, both the intelligence community and the American people have had to adjust to broader and more varied threats in which there are many more players and many more issues involved that affect national security.

To an appreciable degree, our ability to meet these diverse challenges depends on the willingness of the American public to recognize these threats and to support adequate security measures to counter them. Successful security efforts depend on public support for screening and filtering out security threats and for punishing transgressions when preventive strategies have failed.

The Defense Personnel Security Research Center (PERSEREC) undertook to assess the degree of public support for various national security issues. The purpose of this brief management report is to summarize what was learned from PERSEREC's study.[1]

Approach

PERSEREC commissioned the National Opinion Research Center (NORC) at the University of Chicago to include questions on its 1994, 1996, 1998 and 2000 General Social Surveys (GSS). The GSS surveys nationally representative, full-probability samples of adults living in households in the United States.

PERSEREC collected attitude information relative to seven issues:

1. Need for secrecy in various areas of government activity
2. Government's need to collect information on individuals vs. people's privacy rights
3. Public support for various security countermeasures
4. Government's right to know mental health information
5. Loyalty to employer vs. coworkers
6. Punishments for various acts of trust betrayal

[1] NORC's full technical report, with data tables, is available upon request from PERSEREC. Smith, T. W. (2001). Public attitudes towards security and counter-espionage matters: 1994-2000. Chicago: National Opinion Research Center.

7. Perception of threats to the United States

Not every question was asked in each biennial iteration so there is not always a full complement of information for each year. While several items from previous years were omitted in 2000, a number of new questions were asked in 2000 concerning security for information systems and electronic media. Also, responding to concerns that public perception of various threats to national security might be a result of the demise of the Soviet Union, an item was included in 2000 to gauge this sentiment.

Results

The data show that public support for various aspects of national security policy has been relatively stable over several years in taking a strong pro-security stance, although a slight lessening of support is noted for certain areas.

1. Need for Secrecy in Various Areas of Government Activity *(Table A.1, Questions 1-3)*

Although the public consistently believes the government classifies too many documents, it strongly approves maintaining a high level of secrecy surrounding technology with military applications. It also believes that the secrecy of diplomatic initiatives, military operations, and efforts to control domestic terrorism should be protected. However, the public is less supportive of the practice of keeping secret details of the intelligence budget. (These three questions were not repeated in 2000.)

2. Government's Need to Collect Information on Individuals vs. People's Privacy Rights *(Table A.1, Questions 4-6)*

The public supports vetting clearance applicants about various aspects of their lives. Over time respondents have consistently supported the government's right to ask questions about criminal arrests and convictions, illegal drug use, mental health history, and alcohol use. They are less convinced about asking questions about foreign relatives and friends and about financial and credit history, and have consistently given little support to questions concerning sexual orientation. The public responded with strong support to a question, asked for the first time in 2000, about illegal use of computers *(Question 4).*

The public agrees that the government should contact others to verify the information that a clearance applicant supplies. Checking on financial assets and liabilities, the applicant's spouse's finances, and examining tax records are fairly well supported *(Question 5*). The public felt, when queried in 1994, that the government's security rights were more important than individuals' rights to privacy *(Question 6).*

3. Public Support for Various Security Countermeasures *(Table A.1, Question 7)*

In terms of support for various security countermeasures, the public backs all proposed measures to check up on current employees and favors continued checking on employees holding clearances as they move through their careers. However, many object to routine, off-the-job monitoring and wiretapping. Support for on-the-job monitoring and regular questioning about financial matters is also relatively low. For many of these items in 1998 and 2000, a fifth to almost two-fifths neither agreed nor disagreed (not shown in Table A.1) with surveillance, an indication that many people are torn between the goals of protecting secrets and protecting individual rights and privacy.

4. Government's Right to Know Mental Health Information *(Table A.2)*

GSS 2000 responses show continued strong endorsement for the government's right to know about an individual's emotional or mental health. The public approves extensive investigation into mental health histories. This is somewhat at variance with personnel security policy that in recent years has been less intrusive in asking questions about mental health treatment.

5. Loyalty to Employer vs. Coworkers *(Table A.3)*

The public was asked (only in 1994) about what people should do if they saw a person violating security rules. Would they be loyal to their employer—the government—or to their coworker? Respondents were evenly split between those who would immediately report the violation and those who would try to intervene, before reporting, by advising the person to stop the behavior. In other words, they would give the person a chance to change his/her behavior. This is significant, given the fact that cleared individuals are required by regulation to report to authorities any behavior observed among colleagues that may be of security relevance. Presently, the rate of such reporting is extremely low.

6. Punishments for Various Acts of Trust Betrayal *(Tables A.4 - A.5)*

Intelligence-related breaches of trust are seen as serious, and the public favors more punishment in these cases than for offenses involving property theft. Judgments about the seriousness of computer-related security violations (asked for the first time in 2000) depend on the particulars of the crime, with damaging or stealing national security data seen as serious, and unauthorized snooping and downloading pornography as less so.

7. Perception of Threats to the United States *(Table A.6)*

This set of questions on threat perception was included in the GSS for the first time in 2000. While the public is closely divided on whether the threat of nuclear war has grown or diminished over the last 10 years, more people see increased threats from spying, terrorism by US citizens and foreigners, and technology theft.

Trends in Support for Security Measures *(no table)*

Although support for security policy remains high, between 1994 and 2000 there has been a small but general decline in public support for several security measures. The largest declines were for keeping secret technology with military applications, inspection of tax records, verifying personal financial data, verifying financial assets, financial and credit history, sexual orientation, alcohol use, random drug tests, criminal arrests and convictions, mental health history, whether an individual is currently consulting a mental health professional, general nature of the mental health diagnosis, and regular questions about finances. The changes are minor and in no way reach statistical significance.

However, for a few security measures, modest increases in support were noted. These increases involved lie-detector tests, US intelligence budget, and whether an individual had ever consulted a mental health professional. Again, the changes are extremely small.

Conclusions

Without public support for national security measures it would be hard to safeguard and maintain our assets. Ultimately, the people, through their elected representatives, must approve the kind of personnel security system we deploy and the kind of security measures the government imposes. A tension between public and personal rights, and a consciousness of a greater national good, are illustrated in the survey data. It is also clear that the public draws the line at certain invasive techniques that may be used to monitor government employees.

This study shows that between 1994 and 2000 the public has been relatively consistent in its pro-security stance, with only minor shifts in support in recent years in certain areas. When given the choice of backing the government or protecting the personal freedoms of people with security clearances, the public leans towards the government. The public approves the use of seemingly intrusive tests, such as lie detector and random drug tests. In some areas, public approval appears to even outrun security policy itself, as in the case of approving extensive investigation into mental health histories. On the other hand, the public believes that far too much information is being classified. Also, asking questions about people's relatives and friends is not wholly supported, although this is an area deemed by government investigators an important source of information on the person being vetted. The area the public most adamantly opposes is off-the-job monitoring of e-mail and Internet use, a strategy that they clearly consider too intrusive for a democratic society.

On the whole, however, public opinion is congruent with the system in place. This is good news for security awareness professionals charged with the task of instilling into newcomers and longer-term employees alike the ethics, the spirit, and the rules of the present system. An audience so in favor of putting national security ahead of personal rights should, in theory, be a relatively easy target for indoctrination. However, the public has made it clear that not everything can be taken for granted and that, even within the framework of security, there are certain areas, such as monitoring of the home, where government definitely should not venture.

Since the general findings from the GSS have been relatively stable over the past several years, PERSEREC has decided to defer gathering more data, at least for the next few years.

Appendix A

Tables

Appendix A
Table Of Contents

List of Tables

Table A.1
Support for Specific Security Issues: Percentage of Respondent Agreement [a]

	1994	*1996*	*1998*	*2000*
	%	%	%	%
Q1. Government protects too many documents	56	55	55	-
Q2. Government should maintain a high level of secrecy surrounding technology with military uses	76	70	69	-
Q3. Government should maintain a high level of secrecy surrounding:				
Diplomatic initiatives	-	74	74	-
Military operations	-	87	88	-
Efforts to control domestic terrorism	-	83	82	-
US intelligence budget	-	54	56	-
Q4. Government should have the right to ask questions about:				
Financial & credit history	82	79	74	77
Criminal arrests & convictions	98	97	96	96
Illegal drug use	96	96	96	95
Mental health history	95	95	94	93
Foreign relatives & friends	78	79	77	77
Alcohol use	93	93	89	89
Sexual orientation	47	49	44	44
Foreign business contacts	-	-	-	87
Foreign travel	-	-	-	81
Illegal or unauthorized use of computers	-	-	-	93
Q5. Government should contact others to verify information:				
Financial assets & liabilities	-	76	71	-
Spouse's financial assets & liabilities	-	66	62	-
Tax records	-	76	70	-
Q6. Government should protect security above protecting the individual's right to privacy	80	-	-	-

[a] "Strongly agree" and "Agree" responses have been combined.

	1994	*1996*	*1998*	*2000*
	%	%	%	%
Q7. People with security clearances should be subject to the following measures:				
Periodic lie detector tests	-	-	75	78
Random drug tests	-	-	91	88
Wiretapping or electronic surveillance	-	-	38	-
Regular questions about financial assets & liabilities	-	-	49	47
Monitoring at work	-	-	50	-
Monitoring off the job	-	-	43	-
Computer checks of personal financial records	-	-	-	43
Computer checks of international travel records	-	-	-	64
Auditing of e-mail and Internet use at work	-	-	-	64
Auditing of e-mail and Internet use at home	-	-	-	30
Wiretapping of telephone calls at work	-	-	-	45
Wiretapping of telephone calls at home	-	-	-	20
Searches of briefcases and desks at work	-	-	-	48
Video camera surveillance in workplace	-	-	-	64

Table A.2
Government's Right to Know Mental Health Information

	1994	*1996*	*1998*	*2000*
	%	%	%	%
Government has the right to know:				
Nothing about individual's emotional or mental health	-	6	5	6
Whether individual is currently consulting a mental health professional	-	12	12	10
Whether individual has ever consulted a mental health professional	-	8	10	10
Whether individual has ever consulted a mental health professional, and general nature of diagnosis	-	26	27	24
Whether individual has ever consulted a mental health professional, the general nature of diagnosis and counseling, and specific information revealed in confidence to the mental health professional	-	42	38	43
Don't know	-	5	8	7

Table A.3
Loyalty to Employer vs. Coworkers

	1994	*1996*	*1998*	*2000*
	%	%	%	%
When faced with a conflict between loyalty to employer or to coworker who is observed violating security rules, a person should:				
Report coworker to an official	41	-	-	-
Ask coworker to stop, but do nothing further	6	-	-	-
Ask coworker to stop, but report if behavior continues	41	-	-	-
Mind one's own business and not get involved	8	-	-	-
Don't know	4	-	-	-

Table A.4
Serious Punishments Recommended for Various Hypothetical Offenses
(Year 1998 questions)

Offense	*Life imprisonment w/o parole* *%*	*10-20 years* *%*
NCO selling secret codes and other intelligence material to a hostile foreign government	38	35
NCO selling same materials to a friendly foreign government	24	29
Sergeant selling military weaponry to civilians (theft of property)	7	20
Government employee stealing and selling army truck parts to civilians	1	6
High-placed government official leaking sensitive information on a political matter in the media in order to influence public opinion	2	5

Table A.5
Serious Punishments Recommended for Various Hypothetical Offenses
(Year 2000 questions)

Offense	*Life imprisonment w/o parole* *%*	*10-20 years* *%*
Stealing and selling secret codes and other classified information to hostile foreign government	43	30
Stealing and selling secret codes and other classified information to a friendly foreign government	29	28
Intentionally damaging security data on a computer	18	32
Stealing national security data from a computer	18	31
Stealing weapons, ammunitions, and explosives from military depot	18	30
E-mailing secret or top secret government files to an unauthorized person	15	25
Intentionally damaging or destroying a computer system	11	23
	Reprimand	**Firing, or dismissal from military**
Unauthorized snooping into a computer system	6	31
Stealing and selling truck parts and tires from the military	6	28
Leaking serious information to the press to influence public policy, without financial gain	14	40
Downloading pornographic material on an office computer	28	39

Table A.6
Perception of Threats to the United States Compared to 10 Years Ago
(Year 2000 questions)

Offense	*Greater* *%*	*About the same* *%*	*Less* *%*	*Don't know* *%*
Spying by US citizens for foreign countries	31	40	17	12
Spying by foreign agents	35	43	12	11
Terrorism by US citizens	50	26	15	9
Terrorism by foreigners	65	25	6	5
Stealing US advanced technology and trade secrets by foreigners	52	29	7	12
Nuclear war	31	28	32	9